



St. Joseph's Institute of Technology

3rd International Conference on Recent Trends in Engineering and Technology

4th and 5th May 2018

Multi-Factor Authentication Using IMEI Encrypted Color QR Code

Y V V S Sai Pavan, T Lohit Raja, Harini N

Student, Student, Asst Professor, Dept of Computer Science and Engineering, Amrita School of Engineering, Coimbatore. Amrita Vishwa Vidyapeetham, India

{CB.EN.U4CSE15058@cb.students.amrita.edu, CB.EN.U4CSE15053@cb.students.amrita.edu, n_harini@cb.amrita.edu}

ABSTRACT

QR code based technologies have revolutionised the barcode technologies that are prevalent. These have been widely accepted in the literature as practical and interesting data representation model for authentication. The focus of the paper is to design a multi-factor authentication scheme that uses color QR codes for protecting user credentials and study the impact of the model in terms of its capability to mitigate common form of attacks. The experimentation clearly revealed the suitability of the scheme to replace the existing SMS OTP scheme used currently by financial services and E-commerce systems.

Keywords—*Biometrics, Triple Data Encryption Algorithm, Session password, Authentication, Quick Response code, International Mobile Equipment Identity number, Multi-factor, parallel session attack, denial of service attack.*

INTRODUCTION

In this modern world, with all the advancement in technology security has become a major concern. Gone are the days where cracking an 8 digit alphanumeric password is considered hard. With current GPU power, we can crack it in less than 6 hours. So having a single factor authentication is no longer an option. Multi-factor authentication is more secure and reliable when compared to single-factor authentication as we have to provide more than one secret entity. Using biometric authentication as a second factor can increase the security by a large factor since they are unique to an individual. One other problem that is generally faced is remembering the passwords, having a lengthy password can help make the system more secure but will be harder to remember. Here comes the concept of QR codes. One can store the passwords, fingerprints in the form of QR codes. It looks like multi-factor authentication requires the use of multiple QR codes for saving different security entities. An alternative to this is the usage of color QR code that is capable of storing data in multiple layers. Having just QR codes for authentication makes the system vulnerable as anyone can scan and get the details. The system's security is enhanced by encrypting the secret entities with mobiles IMEI number which will be unique to a given handset and then generating colour QR code.

Abbreviations and Acronyms

IMEI: International Mobile Equipment Identity, TDEA: Triple Data Encryption Algorithm, QR: Quick Response.

LITERATURE REVIEW

A. Multi Factor Authentication Scheme

Multi-factor authentication scheme [2] requires more than one user secret entity for authentication which makes the system more secure.

- Factor – 1 Random Generated Session Password. Every session the user tries to login we generate a 32 character alpha numeric session password which can be used only for that session. This makes it hard to brute force the password as they are randomly generated for each session and in worst case scenario if they get revealed it cannot be used to replay new sessions.
- Factor – 2 Biometric Authentication. This relies on biometric factors which are unique to each individual [8,12] and can help in recognising the user and authenticate him/her by comparing the biometric data taken during the registration phase with the data given during login phase. the proposed system uses the fingerprint as a biometric factor. A fingerprint is the impression of ridges on one's finger. They are unique to each person and hence can be used for authenticating an individual. The implementation uses libraries provided by MATLAB to make fingerprint minutiae markings using ridging, thinning and bifurcation. Recorded markings are used in generating a unique number which can be used for authentication.

3rd International Conference on Recent Trends in Engineering and Technology

B. Color QR Code

Barcodes [11,13,14] are widely used in identification but limited storage made their application narrow. QR codes (3D Quick Response codes) provide more storage compared to barcodes. QR codes are available in two forms namely black and white and color QR codes [1,6,7,15,16] have multiple layers to support multiple entities. As the proposed scheme uses multiple factors for providing different security levels, the choice of color QR code will be more suitable than a black and white QR code. If one takes the number of layers as 'n' and the number of factors as 'm' all the 'm' factors could be grouped and ordered into n sets and each set can be stored on the layer of the QR code. To avail enhanced security the layer in the front can store factors of less importance or which could be easily cracked and factors requiring relatively higher importance could be placed in the innermost layers. The proposed system assumes $m=3$ and $n=3$ (red, blue, green) and encodes each of these m factors in those three different layers (red, blue, green). To retain user-friendliness the layers have been merged to create a single color QR code (one scan required for complete authentication). This procedure is illustrated in the Fig.1.

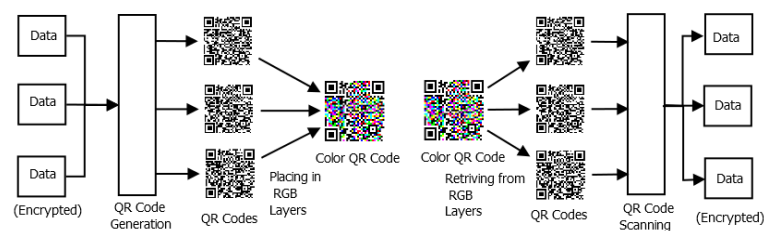


Fig. 1. Encoding and Decoding color QR code

C. Encryption Using Triple Data Encryption Algorithm

Positioning TDEA-Triple Data Encryption Algorithm [3,4,5] is blocked symmetric key cipher which is basically the application of DES thrice. DES (Data Encryption Standard) is a block cipher which takes a 64-bit long block of plaintext and encrypts it using 64-bit long key (actually on 56 bits of the key are used), to produce a 64-bit long ciphertext. The Encryption starts with an initial permutation of 64 bits of plaintext. After this permutation, the block is divided into two 64bit blocks and these two blocks are passed through a function (permutation and substitution are done in the function) where a key is passed as a parameter. 16 such rounds are done and the key for every round is permuted. Finally, the ciphertext will undergo final permutation and the final ciphertext will be produced. Since the text is undergoing several permutations and substitutions the resulting cipher is very difficult to be cracked.

Fig. 2. Example of a figure caption. (figure caption)

D. Tokenless Factor using IMEI number

Literature also specifies the usage of token-less factors for authentication of entities. In this mode, a token which is in possession by the user and not provided by a registration authority is used for authenticating an entity. Normally to enhance security an OTP [9,10] is sent for verification purposes through SMS. The usage of QR code overcomes problems like delay in delivery of SMS and not delivered SMS in the low coverage area, non-availability of the service for roaming users and the downtime with SMS gateway. To restrict and validate that the authentication is done only from the user's token i.e. IMEI number which is unique to every mobile.

SUMMARY OF FINDINGS

Strong authentication has no precise definition. It is only a qualitative measure than a quantitative measure. The strength of an authentication is based on the number of factors used and the trustworthiness associated with each of the factors. An SMS OTP is a very simple idea that can be used as a multi-factor authentication scheme that is still in use by Internet services like electronic banking, E-commerce etc. The following aspects are of relevance here. The mobile network operators cannot guarantee the delivery of SMS within a stipulated time period which will result in expired sessions leading to user frustration. With the exponential increase in the number of people using Internet services for their day to day activities, the above-mentioned problem will be more intensive. This brings out a clear need for a scheme that guarantees authentication without compromise in user friendliness. Work presented in the paper aims at authenticating user with color QR codes.

3rd International Conference on Recent Trends in Engineering and Technology

PROPOSED SYSTEM

The proposed system works in three different phases namely, Registration, Login and Authentication. The model authenticates an entity, based on the possession of the registered mobile phone using its IMEI number to validate the user. The test data as entered by the user in the registration authority premises is shown in Table 1.

TABLE I. REGISTRATION DATA

Type of data	Test Input	Encrypted values(Hex)
Username	alice_anderson1997@gmail.com	1cc97c63196ee4cfe5aa52669e1c57706 514a155e95e6dc385a47eb08f6ea2f0
Session Password	btfVwAcf2XKuaWpKsS5sLnr37Pm8Buhb	527527098fab3a1d602bfe797905cf5aa 1e2275ea239991286177767ecfac1f7
Fingerprint data	22477874629729375939776578287344	49f504dfcd5197b5db9c42a6a3693b53 a3adc53623cf5328cd820f369cceb93

E. Registration Phase

During the registration phase, the user has to provide the email address which will be verified and then asked to provide the fingerprint, after successful scanning of fingerprint a unique fingerprint data is generated and details are stored in the database. Attributes like minutiae position and ridges bifurcation are used in calculating the fingerprint data. Fig.2. depicts the minutiae positions of fingerprint ridges. The user will be requested to add mobile's IMEI number for tokenless authentication and is also added to the database for verification in the later stages. The details are verified by the registration authority and in case of any issues, the registration form is rejected by the authority. This process is shown in Fig.3.

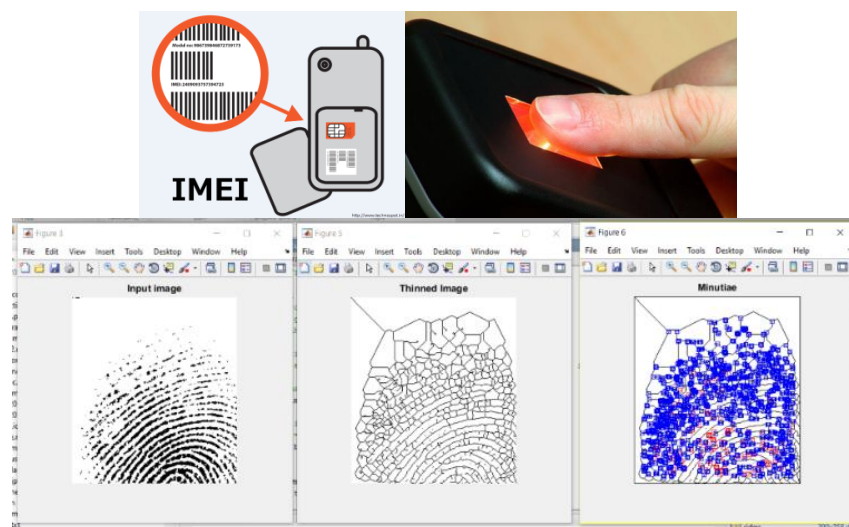


Fig. 3. Minutiae position for fingerprint generated using MATLAB.

F. Login Phase

At the time of availing a service, the user is requested to enter the email ID the server checks the database for the username gets the corresponding unique fingerprint data and generates a random session password. All the three attributes namely username, random session password, and unique fingerprint data are encrypted using TDEA algorithm with IMEI number of the registered mobile as the key. Using these three encrypted entities one can generate three QR codes one for each attribute. These QR codes are digitized in binary form and superimposed into a single image with three layers. The implementation uses the red layer for encrypted username QR code, blue layer for encrypted random session password QR code, green layer for encrypted unique fingerprint data QR code. The one color QR code which is created is displayed to the user on the screen at the time of login which is shown in Fig.5. The user is required to scan the displayed QR code which essentially means submitting credentials for verification. The above process is showed in Fig.4.

3rd International Conference on Recent Trends in Engineering and Technology

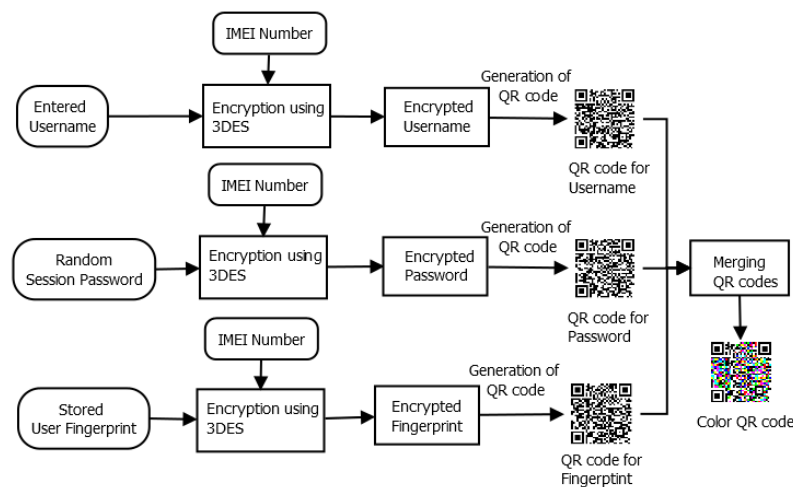


Fig. 4. Working of Login Phase.



Fig. 5. Generated QR codes for Encrypted (A) username (B) Session Password (C) Fingerprint (D) Color QR code.

G. Authentication Phase

The user uses his/her mobile phone to scan the color QR code using the application. It scans the QR code and splits it into three QR codes by separating the three layers (red, blue, green). These three QR codes are then decoded to get the IMEI encrypted [username, random session password, unique fingerprint data]. Application gets the IMEI number of the mobile phone it is installed and uses it to decrypt the encrypted [username, random session password, unique fingerprint data] with TDEA algorithm and sends [username, random session password, unique fingerprint data] to the server and the server verifies them with the values stored in database at the registration server and provides the authentication accordingly. Fig.6 illustrates the above process, and the data is showed in Table 2. Fig.7 shows the screenshot of the mobile while scanning followed by the image captured by the mobile and then the three separated layers generated using MATLAB.

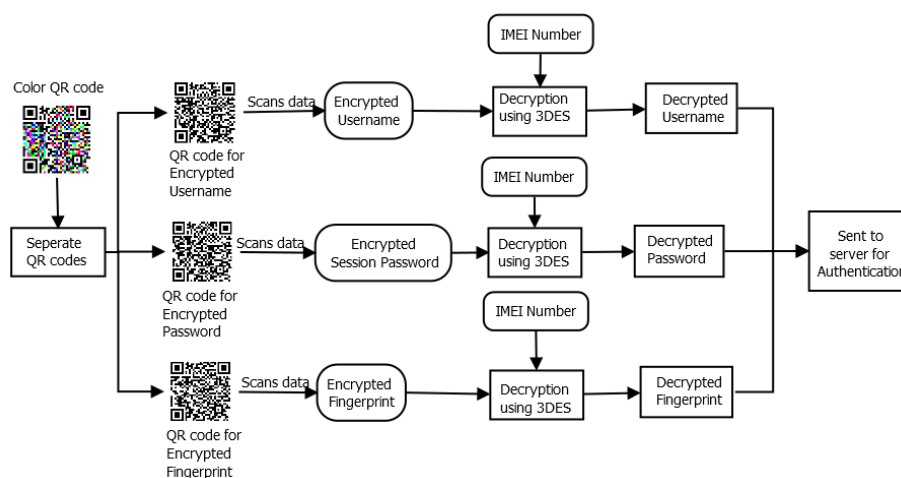


Fig. 6. Working of Authentication Phase.

3rd International Conference on Recent Trends in Engineering and Technology

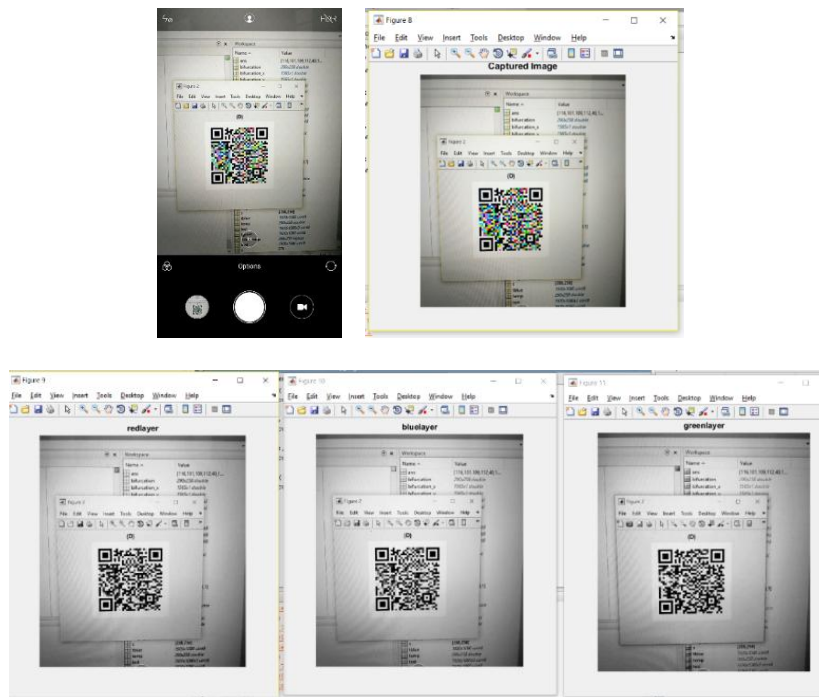


Fig. 7. Testing of Authentication Phase.

TABLE II. DATA FOR AUTHENTICATION

Scanned data	Data after Decryption	Authentication
1cc97c63196ee4cfe5aa52669e1c5770 6514a155e95e6dc385a47eb08f6ea2f0	alice_anderson1997@gmail.com	Verified
527527098fab3a1d602bfe797905cf5a a1e2275ea239991286177767ecfac1f7	btfVwAcf2XKuaWpKsS5sLnR37Pm8Buhb	Verified
49f504dfcd5197b5db9c42a6a3693b53 a3adc53623cf5328cd820f369cceb9f3	22477874629729375939776578287344	Verified

H. Reliability of Scheme

Sessions on Internet service transactions are usually short-lived. The usage 32 character random generated session password which makes it almost impossible to crack since it takes years to crack. This makes the system strong against password cracking employing brute force. The usage of fingerprint data for authentication prevents a sniffer from obtaining the actual fingerprint. As only the computed fingerprint is available on the server which is generated based on one way it is impossible for an attacker to get the original fingerprint data. The scheme also facilitates the user to use a lengthy password as it does not require him/her to remember the password.

- Scenario-1: Valid user requesting verification. In this scenario, the user scans the color QR code which is separated to get the encrypted entities. His/her IMEI number is used to decrypt the separated entities which are sent to the server for authentication. If the procedure mentioned in section 4.3 succeeds the user is authenticated.
- Scenario-2: An attacker performing parallel session attack. In this case, an attacker tries to impersonate the legitimate user by intercepting login request. The attempt would fail as per the proposed scheme as the attacker would not own the mobile phone of the user which is very required for decrypting entities separated.
- Scenario-3: Resistance to denial of service attack. The system blocks after three failed attempts and the failure would lead to blocking the user data in the registration database. The legitimate user needs to contact the registration authority for enabling his/her account.

3rd International Conference on Recent Trends in Engineering and Technology

CONCLUSION

This paper proposes a multi-factor authentication scheme based on color QR code verification mechanism rather than SMS based OTP which is commonly used in web and mobile application. The proposed model clearly brings out the capabilities of the scheme in terms of its strength to mitigate forms of common attacks like parallel session attack, replay attack, brute force attack. With the available smartphone architectures capable of scanning QR codes the system prevents the requirement of additional hardware. The proposed system was tested using penetration tools to analyze, quantify, measure the resistivity offered to mitigate the above-mentioned security risks. It is planned to enhance the model with the use of public key cryptosystems as a future extension.

References

- [1] Aryachandran S, Jyothi R L, "Secure Color QR codes", IOSR Journal of Computer Engineering (IOSR-JCE) e-ISSN: 2278-0661, p-ISSN: 2278-8727, PP 77-85.
- [2] Tushar Bhivgade , Mithilesh Bhusari , Ajay Kuthe , Bhavna Jiddewar , Prof. Pooja Dubey, "Multi-factor Authentication in Banking Sector", Tushar Bhivgade et al, / (IJCISIT) International Journal of Computer Science and Information Technologies, Vol. 5 (2) , 2014, 1185-1189.
- [3] Yang Jun Li Na Ding Jun, "A design and implementation of high-speed 3DES algorithm system", 2009 Second International Conference on Future Information Technology and Management Engineering.
- [4] Shaify Kansal, Meenakshi Mittal, Performance, "Evaluation of Various Symmetric Encryption Algorithms", 2014 International Conference on Parallel, Distributed and Grid Computing.
- [5] Dr T.R Padmanabhan, N.Harini and Dr.C.K.Shyamala, "Cryptography and security", WileyIndia, First Edition, 2011.
- [6] Zhibo Yang, Huanle Xu, Jianyuan Deng, Chen Change Loy and Wing Cheong Lau, "Robust and Fast Decoding of High-Capacity Color QR Codes for Mobile Applications", arXiv:1704.06447v2 [cs.CV] 30 Jan 2018.
- [7] Jeng-An Lin, Chiou-Shann Fuh, "2D Barcode Image Decoding" Hindawi, vol. 1, 2013.
- [8] Sajan Ambadiyila , K S Soorej, V P Mahadevan Pillaic, "Biometric based Unique ID Generation and One to One Verification for Security Documents", International Conference on Information and Communication Technologies (ICICT 2014).
- [9] Swapnoneel Roy, Matt Rutherford, Charlene H. Crawshaw, "Designing and implementing a secure one time password (OTP) authentication system", 2016 IEEE 35th International Performance Computing and Communications Conference (IPCCC) (2016).
- [10] ByungRae Cha, ChulWon Kim "Password Generation of OTP System using Fingerprint Features", 2008 International Conference on Information Security and Assurance (ISA '08) (2008).
- [11] Tobias Marktscheffel , Wolfram Gottschlich , Wolfgang Popp , Philemon Werli , Simon Dominik Fink , Hermann de Meer , "QR code based mutual authentication protocol for Internet of Things", (2016) to ISSN:, ISBN: , pp: 1-6.
- [12] Prasad K Saralaya, R Anjali, G Shivaprasad, N V Subba Reddy, "Biometric Authentication Usage for Internet Banking", Recent Trends in Electronics, Information & Communication Technology (RTEICT), 2017 2nd IEEE International Conference on 19-20 May 2017.
- [13] Information Technology-Automatic Identification and Data Capture Techniques-QR Code 2005 Bar Code Symbology Specification. (2011, Jan.) [Online].
- [14] A. Grillo, A. Lentini, M. Querini, and G. F. Italiano, "High capacity colored two dimensional codes", in Proc. Int. Multiconf. Comput. Sci. Inf. Tech., Oct. 2010, pp. 709a-716.
- [15] M. Querini, A. Grillo, A. Lentini and G. F. Italiano, "2D Color Barcodes For Mobile Phones", International Journal of Computer Science and Applications Techno mathematics Research Foundation Vol. 8 No. 1, pp. 136 - 155, 2011.
- [16] Dr. Senthil Kumar M., Aishwarya, M., K. Vaishnavi, S., Sukanya, R., Aiswariya, C., and Dr. Harini N., "An Improved Authentication Scheme Using Colour QR Codes", in Proceedings of International conference on Adaptive Technologies for Sustainable Growth (ICATS-2014), 2014.
- [17] R. Joseph Manoj, M.D. Anto Praveena, K. Vijayakumar, "An ACO-ANN based feature selection algorithm for big data", Cluster Computing The Journal of Networks, Software Tools and Applications, ISSN: 1386-7857 (Print), 1573-7543 (Online) DOI: 10.1007/s10586-018-2550-z, 2018.
- [18] G. Indrajith and K. Vijayakumar, "Automatic Mathematical and Chronological Prediction in Smartphone Keyboard" International Journal of Engineering and Computer Science ISSN: 2319-7242 Volume 5 Issue 5 May 2016, Page No. 16714-16718.

